Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A method of encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, the method comprising:

obtaining a source stream;

identifying a first set of blocks of said source stream as secure blocks;

identifying a second set of blocks of said source stream as unsecure blocks;

encrypting said secure blocks using each of a plurality of keys for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destinations systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class; and

grouping said unsecured blocks and the plurality of encrypted versions of secured blocks as the common data stream.

2. (Original) The method of claim 1, wherein said source stream is packetized video data.

3. (Original) The method of claim 1, further comprising encrypting unsecure blocks such that said unsecure blocks are decryptable by each of said plurality of destination systems, if authorized by at least one conditional access system.

4. (Original) The method of claim 1, wherein encrypting comprises encryption utilizing at least one of AES, with at least one AES key per class of destination systems, and DES, with at least one DES key per class of destination systems.

5. (Original) The method of claim 1, wherein said blocks are MPEG blocks and said secure blocks represent MPEG I frames.

6. (Currently amended) A method, in a destination system, of decoding a common data stream distributed to a plurality of destination systems, said method comprising:

obtaining said common data stream, wherein said common data stream includes a plurality of encrypted versions of secure blocks and unsecure blocks of data, said encrypted versions of secure blocks being encrypted, using each of a plurality of keys, for each of a plurality of classes of destination systems, respectively;

decrypting only a portion of said encrypted versions of secured blocks that is encrypted using at least one key associated with a class of the destination system, thereby forming decrypted secure blocks; and

grouping said unsecure blocks and said decrypted secure blocks as a useful stream for use by said destination system.

7. (Original) The method of claim 6 further comprising demultiplexing said common data stream into secure and said unsecure blocks.

8. (Original) The method of claim 6, wherein decrypting comprises decryption utilizing at least one of AES, with at least one AES key per class of destination systems, and DES, with at least one DES key per class of destination systems.

9. (Currently Amended) The method of claim 6 further comprising providing at least one decryption key for said step of decrypting.

10. (Currently Amended) The method of claim 6 further comprising discarding a portion of said encrypted versions of secured blocks that is encrypted using at least one key not associated with the class.

11. (Original) The method of claim 6, wherein said blocks are MPEG blocks and said secure blocks represent MPEG I frames.

12. (Currently Amended) An encoder system for encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, said encoder system comprising:

an input for receiving a source stream;

an encoder, said encoder receiving said source stream and packetizing said source stream to provide a plurality of packets; and

an encryptor for selectively identifying at least one set of blocks of said packets as secure blocks and encrypting said secure blocks, using each of a plurality of keys, for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destination systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class.

13. (Currently Amended) The encoder system of claim 12, wherein said encryptor combines said encrypted versions of secured blocks and said unsecure blocks to form a common data stream.

14. (Original) The encoder system of claim 12, wherein said encoder is an MPEG encoder.

15. (Original) The encoder system of claim 12, wherein said encryptor is at least one of a DES encryptor and an AES encryptor.

16. (Currently Amended) An encoder system for encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, said encoder system comprising:

an input for receiving a source stream;

an encoder, said encoder receiving said source stream and packetizing said source stream to provide a plurality of packets;

encryption selector for selectively identifying at least one set of blocks of said packets as secure blocks; and

an encryptor for encrypting said secure blocks, using each of a plurality of keys, for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destination systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding.

17. (Currently Amended) The encoder system of claim 16, wherein said encryptor combines said encrypted versions of secured blocks and said unsecure blocks to form a common data stream.

18. (Original) The encoder system of claim 16, wherein said encoder is an MPEG encoder.

19. (Original) The encoder system of claim 16, wherein said encryptor is at least one of a DES encryptor and an AES encryptor.

20-23. (Canceled)

24. (Currently Amended) A content transport system, comprising:

a selector for selecting blocks to be encrypted as secure blocks;

a secure block multi-encryptor, for encrypting said secure blocks, using each of a plurality of keys, for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destination systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class;

a combiner for combining unsecure blocks and encrypted versions of secured blocks into a common stream;

a demultiplexer for separating said common stream into blocks that are usable by a destination system and blocks that are not usable by the destination system;

a selective decryptor that decrypts usable version of secured blocks; and

a reassembler for reassembling a useful signal stream from any unsecure blocks, and said version of secured blocks decrypted by the selective decryptor, wherein an ability to reassemble the useful signal stream relies in part on an ability to decrypt usable version of secured blocks.

25. (Original) The system of claim 24, wherein the reassembler is an MPEG decoder.

26. (Currently Amended) A computer-readable medium that is a physical memory storage device, the computer-readable medium including a common data stream comprising:

a plurality of secure blocks encoded from a source stream, said plurality of secure blocks encrypted, using each of a plurality of keys, for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destination systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class; and

27. (Currently Amended) A computer-readable medium that is a physical memory storage device, the computer-readable medium including computer program instructions for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream that instruct a computer to perform the steps of.

obtaining a source stream;

identifying a first set of blocks of said source stream as secure blocks;

identifying a second set of blocks of said source stream as unsecure blocks;

encrypting said secure blocks, using each of a plurality of keys, for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destination systems, thereby forming a plurality of encrypted versions of encrypted secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class; and

grouping said unsecured blocks and the plurality of encrypted versions of secured blocks as the common data stream.

28. (Currently Amended) A computer-readable medium that is a physical memory storage device in a destination system, the computer-readable medium including computer program instructions for decoding a common data stream distributed to a plurality of destination systems, that instruct a computer to perform the steps of:

obtaining said common data stream, wherein said common data stream includes a plurality of encrypted versions of secure blocks and unsecure blocks of data, said encrypted versions of secure blocks being encrypted, using each of a plurality of keys, for each of a plurality of classes of destination systems, respectively;

decrypting only a portion of said encrypted version of secured blocks that is encrypted using at least one key associated with a class of the destination system, thereby forming decrypted secure blocks; and

grouping said unsecure blocks and said decrypted secure blocks as a useful stream for use by said destination system.

29. (New) The method of claim 1, wherein the first set of blocks and the second set of blocks are identified in accordance with a desired ratio as indicated by a control parameter.

30. (New) The method of claim 6, wherein the portion of said encrypted versions of secured blocks includes at least one encrypted version of secured blocks among the plurality of encrypted versions of secured blocks.